TITLE:

Friend-to-friendオーバーレイネットワークにおける効率的な分散ルーティング (複雑コミュニケーションサイエンス)

AUTHOR(S):

髙橋, 彰; 宮崎, 修次

CITATION:

髙橋, 彰 ...[et al]. Friend-to-friendオーバーレイネットワークにおける効率的な分散ルーティング (複雑コミュニケーションサイエンス). 電子情報通信学会技術研究報告 2017, 116(514): 13-18

ISSUE DATE:

2017-03-03

URL:

http://hdl.handle.net/2433/254185

RIGHT:

Copyright ©2017 by IEICE

京都大学学術情報リポジトリ
KURENAI 紅
Kyoto University Research Information Repository

京都大学 KYOTO UNIVERSITY
A Self-archived copy in
Kyoto University Research Information Repository
https://repository.kulib.kyoto-u.ac.jp
京都大学学術情報リポジトリ KURENAI 紅 Kyoto University Research Information Repository

一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
CCS2016-47 (2017-03)

Friend-to-friend オーバーレイネットワークにおける効率的な分散ルーティング

髙橋　彰† 宮崎　修次††

† 京都大学工学部情報学科 〒606–8501 京都市左京区吉田本町
†† 京都大学情報学研究科 〒606–8501 京都市左京区吉田本町
E-mail: †takahashi.akira.58s@kyoto-u.jp, ††syuji@acs.i.kyoto-u.ac.jp

あらまし　Friend-to-friend (F2F) ネットワークは，各ノードが信頼のおける特定ノードとのみ通信を行う特殊な P2P ネットワークであり，Freenet 等の検閲に対する耐性を重視したコミュニケーションシステムの基礎となっているが，ネットワーク上でのルーティングパフォーマンスが低いという問題点を抱えている．本研究では，次ノード選択時に隣接ノードの次数に応じた重み付けを行うというアプローチから，Freenet で用いられているルーティング手法を改良する．そしてスモールワールド性とスケールフリー性を持った信頼関係ネットワークである Web of Trust におけるルーティングのシミュレーション実験を行ったところ，今回提案するアルゴリズムが既存の Freenet におけるルーティングアルゴリズムよりも高いパフォーマンスを発揮することを確認した．
キーワード　friend-to-friend, 分散ルーティング，複雑ネットワーク

Efficient decentralized routing in friend-to-friend overlay networks

Akira TAKAHASHI† and Syuji MIYAZAKI††

† Undergraduate School of Informatics and Mathematical Science, Faculty of Engineering, Kyoto University
Yoshida-Honmachi, Sakyo-ku, Kyoto, 606–8501, Japan
†† Graduate School of Informatics, Kyoto University Yoshida-Honmachi, Sakyo-ku, Kyoto, 606–8501, Japan
E-mail: †takahashi.akira.58s@kyoto-u.jp, ††syuji@acs.i.kyoto-u.ac.jp

Abstract　Friend-to-friend (F2F) networks, connectivity-restricted P2P networks which provide censorship-resistant communication systems such as Freenet, suffer from a poor routing performance. In this paper, we improve Freenet's routing algorithm by utilizing neighbors' degree information in message forwarding. Our routing simulations in PGP Web of Trust, a real-world trust relationship network with small-world and scale-free characteristics, show that the proposed method outperforms the existing routing algorithm of Freenet.
Key words　friend-to-friend, decentralized routing, complex network

1. はじめに

近年インターネットを介したコミュニケーションまたは出版は，我々の生活において大きな位置を占めるようになってきた．それに伴いユーザーのプライバシー保護を重視したコミュニケーションツールの実装に対する需要が非常に高まっている．その要因として，例えば近年では Snowden によって公に明らかにされたアメリカ国家安全保障局 (NSA) による大規模な大衆監視が挙げられる [1].

特定の企業や団体が中央集権的に管理する情報共有方式は検閲・漏洩のリスクが高いため，非中央集権的な情報共有を実現するためのアプローチとして P2P 方式が頻繁に採用される．P2P 方式にも様々なタイプがあるが，その中でも friend-to-friend (F2F) [2] は特にピアの匿名性・プライバシー保護に重点を置いたネットワーキング方式であり，F2F ネットワークにおいて各ノードは，信頼のおける特定ノードとのみ通信する．F2F 方式では，分散ハッシュテーブル (DHT) 等とは異なり，動的にネットワーク構造を最適化することはできず，ネットワーク構造は常に現実の信頼関係ネットワークの部分グラフに対応する．そしてネットワーク上で隣接していないノード同士がデータの送受信を行うためにはいずれかのノードが「知り合いの知り合い」を辿って他方のノードに到達するための経路を探索する必要性が生じる [3], [4].

This article is a technical report without peer review, and its polished and/or extended version may be published elsewhere.
Copyright ©2017　by　IEICE

京都大学 KYOTO UNIVERSITY
A Self-archived copy in
Kyoto University Research Information Repository
https://repository.kulib.kyoto-u.ac.jp
京都大学学術情報リポジトリ KURENAI 紅 Kyoto University Research Information Repository

F2F オーバーレイネットワークの最も代表的な実装例は，Freenet [5] の F2F モード [6] であり，基本的なプロトコルは Sandberg が 2006 年に提案した手法 [7] に基づいている．Freenet では，信頼関係のネットワークがスモールワールド性を持つと仮定し，エッジ生成確率が以下の式 (1) のようにノード間の距離に反比例する Kleinberg のスモールワールドネットワークモデル [8] が用いられている．ただし $d(u,v)$ は特定の距離空間に配置されたノード u,v 間の距離，Z は正規化定数で，$Z = \sum_{v \in V, v \neq u} d(u,v)^{-1}$ である．

$$p(u,v) = \frac{1}{d(u,v)Z} \tag{1}$$

Kleinberg モデルにおいて，単純な greedy ルーティング (各ノードは隣接ノード中，最もターゲットに近いノードを次ノードとして選択) によるホップ数期待値が $O(\log^2 n)$ であることが証明されているため，Freenet においては Kleinberg モデルの特徴を反映するように各ノードに対して座標情報を付与することでルーティングの効率化が図られている．

ただし Freenet には未だ様々な問題点が残っている．第一に Sandberg が提案した手法では，Kleinberg モデルの特徴を正確には反映することができないため，Freenet の実装においては greedy ルーティングの代わりに distance-directed depth-first search (D^2-DFS) が採用されている．しかしこのルーティングアルゴリズムの効率性は保証されておらず，結果として実際にデプロイされた Freenet の F2F モードにおけるデータ探索のパフォーマンスは低い．また Freenet では，ノードへの ID 割り当てアルゴリズムの一環としてノード同士が ID を交換するが，この際悪意のあるノードが虚偽の ID 報告を繰り返すことにより，ノードが ID 空間上に偏在し，結果的にルーティングの効率性が低下するという Pitch black attack [9] などの深刻な脆弱性が指摘されている．よって Freenet の F2F モードは効率性や頑健性の面で問題点が残り，現在もそれらを解決するための研究が続けられている．

本研究では，以上に挙げられた Freenet の問題点のうちルーティングの効率性に着目する．今回我々は Şimşek, Jensen らによって提案された expected-value navigation (EVN) [10] のヒューリスティックを利用し，次ノード選択時に隣接ノードの次数に応じた重み付けを行うというアプローチから，Freenet で用いられているルーティング手法を改良することを試みた．また，先行研究のシミュレーション実験においてはルーティングの成功率が向上するように実データの恣意的な改変が施されていたが，本研究では改変を施さない実データに対するシミュレーション実験を行うことにより，現実の F2F トポロジーにより近いネットワークにおけるルーティングアルゴリズムのパフォーマンス評価を行った．

2. Freenet プロトコル

本節では Freenet の F2F モード (または Darknet モードとも呼ばれる) の概略について述べる．F2F モードの目的は P2P システムにおけるノードのプライバシー保護であり，ネットワーク上の各ノードは予め信頼のおけるノードとのみ直接の通信を行う．つまり「友人と友人」(friend-to-friend) の通信のみを行うという制約を設けることによって，信頼関係の外部にいる攻撃者によるプライバシー侵害を困難にしようというのが核心となるコンセプトである．

この制約があるため，F2F モードにおいては通信効率を最適化するようにネットワークトポロジー自体に変更を加えることが不可能であり，各ノードはネットワークの全体像も把握することができない．よって，ネットワーク上で隣接していないノードどうしがデータの送受信を行うためには，Milgram のスモールワールド実験 [11] のようにネットワーク上の中継ノードが局所的な情報のみを用いてメッセージのフォワーディングを繰り返す必要がある．

そこでネットワークトポロジーを変えずにルーティングを効率化するために F2F モードが取るアプローチが，ネットワークの ID 空間への「埋め込み」(embedding) である．埋め込みとルーティングの概念図を図 1 に示す．

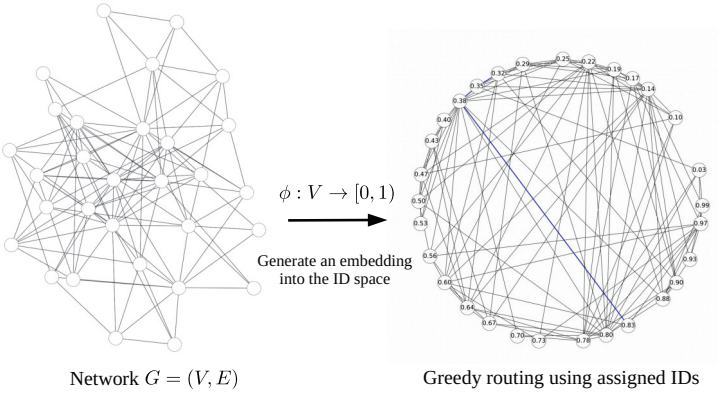

図 1　Freenet の F2F モードにおける埋め込みとルーティングの概略

一般的にネットワーク $G = (V, E)$ の距離空間 (X, d) への埋め込みは単射 $\phi : V \to X$ で定義される [12]．Freenet では以下の式 (2) で定義される距離関数 d を備えた単位区間 $[0, 1)$ が上記の X に対応し，ID 空間 (ID space) またはキー空間 (key space) などと呼ばれる．以下では空間上の一点を便宜的に “ID” または「座標」と呼ぶこととする．図 1 のように ID 空間上の各点は円上の点に，2 点間の距離は円周上の距離に対応付けることができる．

$$\forall x, y \in [0,1), d(x,y) = \min\{|x-y|, 1-|x-y|\} \tag{2}$$

よって F2F モードでは，効率的な分散ルーティングが可能となるように ID 空間への埋め込み ϕ を生成することが重要となる．

2.1 ネットワークの埋め込み

埋め込みの生成は Sandberg が 2006 年に提案した手法 (以下 SWAP アルゴリズムと呼ぶ) に基づいている [7]．SWAP アルゴリズムは埋め込みの生成をパラメータ ϕ の推定問題として

京都大学 KYOTO UNIVERSITY
A Self-archived copy in
Kyoto University Research Information Repository
https://repository.kulib.kyoto-u.ac.jp
京都大学学術情報リポジトリ KURENAI 紅 Kyoto University Research Information Repository

みなし, ID 空間に埋め込まれたグラフが Kleinberg のスモールワールドモデルによって生起する確率が高くなるように (つまり ID 空間において隣接するノード間の距離の分布が式 (1) に従うように), ϕ を Metropolis-Hastings 法によりサンプリングする.

SWAP アルゴリズムの概略は以下の通りである.

（0） 各ノードは $[0,1)$ 上の一様乱数を発生させ, 初期 ID を得る. これを初期状態とする.

（1） ノード u は ID 交換相手の候補 v をネットワーク上でのランダムウォークにより選択し, ID 交換リクエストを送る.

（2） 各 u,v がそれぞれ「隣接ノードと自分の距離」「隣接ノードと相手の距離」を計算することで, 採択確率 $\beta(\phi_1,\phi_2)$ を得る. ただし ϕ_1 は現在の埋め込みのサンプル, ϕ_2 は候補サンプルで, ϕ_1 における u,v の ID 割り当てを入れ替えたものである.

（3） $[0,1)$ 上の一様乱数を生成し乱数が $\beta(\phi_1,\phi_2)$ を超えなければ, u,v は ID を交換, すなわち埋め込みの候補サンプル ϕ_2 を採択し, さもなくば ID 交換を行わない.

以上の (1) から (3) までの操作を十分な回数反復することで, greedy ルーティングによる平均ホップ数が短くなるような ID の割り当てを生成することができる. Sandberg は人工的に生成した Kleinberg のネットワークデータと実データに対してシミュレーション実験を行い, SWAP アルゴリズムの適用後割り当てられた座標情報が, ランダムに割り当てられた座標情報に比して greedy ルーティングの効率性を高めることを示した.

2.2 ルーティングアルゴリズム

SWAP アルゴリズムの適用は確かに greedy ルーティングの効率性を高めるような ID の割り当てが可能であるが, 本来の Kleinberg モデルと同様の $O(\log^2 n)$ のホップ数は保証されない. なぜなら, Kleinberg モデルでは空間上で最も距離の近いノードへのエッジ (local contact) が必ず存在しているという仮定によって greedy ルーティングの最中にターゲットまでの距離が狭義に単調減少することが保証されているが, SWAP アルゴリズムによって ID 空間に埋め込まれたネットワークは必ずしもこの local contact を持たないからである. よって単純な greedy ルーティングでは “dead-end”(自分よりもターゲットに近い隣接ノードが存在しない状態) に達してしまう. そこで Freenet では単純な greedy ルーティングではなく, ホップ数上限付の distance-directed depth-first search (D^2-DFS) を採用することで dead-end に対処している [5]. D^2-DFS は dead-end に陥った場合でもターゲットから遠ざかることを許し, 隣接ノード中最もターゲットに近いものを選ぶという点と, 隣接ノードが全て訪問済みの場合には自らに初めてメッセージをフォワードしたノード (predecessor) にメッセージを戻す (つまりバックトラッキングを行う) という点において異なる. D^2-DFS の動作例を図 2 に示す.

ただし D^2-DFS は dead-end から脱出して greedy ルーティングを継続するための戦略に過ぎないのでルーティングの効率性向上に寄与するものではない. 実際近年 Roos, Strufe らは local contact の存在を仮定しない修正 Kleinberg モデルを

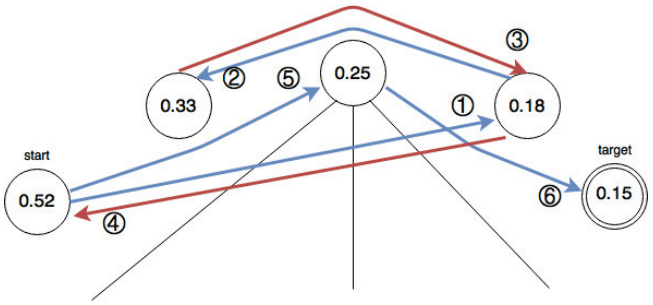

図 2 D^2-DFS の動作例: ソースノード ID 0.52, ターゲットノード ID 0.15 の場合

提案し, そのようなグラフにおいて D^2-DFS がポリ対数関数 (polylogarithmic) のオーダーでルーティングを終えることができないことを解析的に証明した [13].

3. 問題設定

2. 節に述べた F2F ネットワークにおける分散ルーティング効率を向上させるための大まかな方針として (i) 埋め込みアルゴリズムの改良 (ii) 分散ルーティングアルゴリズムの改良 の 2 通りを挙げることができるが，本研究では後者の方針を取る．そこで今回我々は Freenet プロトコルにおける埋め込みアルゴリズムの不正確さに対処するために，F2F ネットワークの実データが持つスケールフリー性に着目し，次ノード選択時に隣接ノードの次数に応じた重み付けを行うルーティングアルゴリズム提案する．なぜなら次数の高いノードに優先的にメッセージをフォワードすれば，隣接ノードが全て訪問済みなるといった状況を避けやすく，バックトラッキングのような無駄なステップを省略できると予想されるからである．このアイデアを検証するため，D^2-DFS を改良したルーティングアルゴリズム, degree-and-distance-directed depth-first search (D^3-DFS) の提案と, 実データを用いたパフォーマンス評価を行っていく.

4. 提案アルゴリズム

まず D^3-DFS において用いるヒューリスティックスを定義するために，隣接ノードの次数とノード間の同類性 (homophily) を考慮した expected-value navigation(EVN) [10] におけるヒューリスティックの枠組みを用いる.

EVN の基本的なアイデアは, メッセージを持っているノード u の隣接ノード v からターゲットノード t までの経路長 $l(v,t)$ を考え, その期待値を近似的に $E(l(v,t)) \approx 1 - e^{k_v p(v,t)}$ とおき，$E(l(v,t))$ を最小化するような v を次ノードとして選択するというものである. ただし k_v を v の次数, $p(v,t)$ を v から t へのエッジが生成される確率とする.

よってある v が $E(l(v,t))$ を最小化することは, $1/k_v p(v,t)$ を最小化することと同値であるからヒューリスティック関数 $f(v)$ を

$$f(v) = \frac{1}{k_v p(v,t)} \tag{3}$$

と定義すれば，「メッセージを持つノード u は (3) 式で定義さ

京都大学 KYOTO UNIVERSITY
A Self-archived copy in
Kyoto University Research Information Repository
https://repository.kulib.kyoto-u.ac.jp
京都大学学術情報リポジトリ KURENAI 紅 Kyoto University Research Information Repository

れる $f(v)$ を最小化するような v にメッセージをフォワードする」というシンプルなルーティングアルゴリズムにより，「隣接ノード中ターゲットまでのホップ数が最も少ないと期待されるノード」を選択することができる．

以上に述べた EVN のヒューリスティックを Freenet プロトコルに応用するためには，Kleinberg モデルに従ってエッジが生成されたと仮定した場合の $p(v,t)$ を代入すれば良い．つまり ID 空間 $[0,1)$ 上にノードを持つネットワークのエッジが Kleinberg モデルに従って生成されたと仮定すると隣接ノード v がターゲットノード t と隣接する確率は (1) 式より，$p(v,t) = 1/d(v,t)Z$ であるから，これを (3) 式に代入するとヒューリスティック関数は $f(v) = d(v,t)Z/k_v$ と表すことができる．

ここで，ノードの ID が SWAP アルゴリズムに従って生成された場合，ID は $[0,1)$ 上に一様に分布しており，その場合正規化定数 Z は任意のノードについて同じ値であると見なすことが出来る．よってヒューリスティック関数の大小比較のみをするのであれば Z の計算は省略可能である．ヒューリスティック関数を改めて $g(v)$ とすれば

$$g(v) = \frac{d(v,t)}{k_v} \tag{4}$$

よって D^3-DFS において，u は (4) 式を最小にするような v にメッセージをフォワードすることが基本的な動作となる．これは通常の距離のみを用いた greedy ルーティングに次数の重み付けを付加したものと見なすことができる．

次に，u の全ての隣接ノードが以前にメッセージを受け取ったことがあるような状況を考える．このような場合 Şimşek, Jensen らは，次ノードを隣接ノードの中からランダムに選択することが最適であると結論づけているが，ランダムなノード選択では同様に隣接ノードが全て訪問済みであるようなノードに何度も到達する可能性があり無駄なステップが増えることが予想されるため，D^3-DFS では D^2-DFS と同様，u に初めてメッセージをフォワードしたノード (predecessor) にメッセージを戻すとする．

最後に D^3-DFS において各ノードが利用可能な情報をまとめると以下のようになる．

- 自分と隣接ノードの ID
- ターゲットの ID
- 隣接ノードの次数

上記の最初の 2 つは Freenet における D^2-DFS が利用する情報と同様であるが，隣接ノードの次数は新たに追加された情報である．実際の F2F ネットワークにおける実装においては，各ノードが互いに現在の接続ノード数に関する情報を隣接ノードと共有し合う状況ということになる．隣接ノードの単なる次数情報はグラフ全体のトポロジーを明らかにするものではなく，信頼するノード以外に対してアイデンティティを明かすことにもなりえないため，D^3-DFS はプライバシーコントロールやセキュリティ面を重視する Freenet などの F2F ネットワークに十分適用可能であると考えられる．

5. 評　　価

5.1 シミュレーション手法

D^3-DFS のパフォーマンス評価を行うために 5.2 節で述べる実データに対するシミュレーション実験を行った．実験の基本的な流れは先行研究と同様 (i) 埋め込みの生成 (ii)ID 空間における分散ルーティングの実行 という 2 つのステップから成る．

(i) においては 2. で述べた Sandberg の埋め込みアルゴリズムを適用し，各ノードに対する ID の割り当てを行った．ただし，[7] に従い Metropolis-Hastings アルゴリズムの反復を $6000|V|$ 回，[4] に従い SWAP アルゴリズムにおけるランダムウォークの試行回数を 10 と設定した．

ID 割り当ての終了後，(ii) においては全てのノードを出発点として，各ノードにつき 5 つのターゲットノードをランダムに選びルーティングのシミュレーションを行った．ただし [7] や [14] に従いルーティングの寿命 (time-to-live)$TTL \approx \log^2 |V|$ とし，1 ホップをカウントするごとに TTL を 1 減らし，$TTL = 0$ となった時点でルーティングを失敗とみなした(注1)．なお以下ではルーティングの「成功率」を (TTL が 0 になる前にターゲットの探索が完了したルーティング試行の数)/(全ルーティング試行の数) として定義する．

以上の条件下で $5|V|$ 回 D^3-DFS のルーティングシミュレーションを行い，ルーティングの成功率，成功したルーティング試行の平均ホップ数を集計した．また比較のために D^2-DFS アルゴリズムに対しても同様の実験を行った．

また成功率の異なるルーティングアルゴリズム間で平均ホップ数の大小を比較するのは不適切であるため，TTL を長めに (恣意的ではあるが本研究では 500 とする) 設定してルーティング実験を同様に $5|V|$ 回行った場合の「各ホップ数以下で成功したルーティング試行の割合」を集計した．

5.2 使用データ

F2F ネットワークに関わる先行研究の多くは埋め込みやルーティングアルゴリズムのパフォーマンス評価のため，実世界のソーシャルネットワークデータを使用している．なぜなら Freenet のような実際にデプロイされている F2F ネットワークはその性質上ネットワーク全体のトポロジーを把握することが不可能であり，代わりに信頼関係を表すソーシャルネットワークデータが F2F ネットワークトポロジーを近似するものと考えられるからである．本研究もそれに倣い F2F ネットワークの実データとして，2016 年 12 月 11 日時点における Pretty Good Privacy (PGP) の Web of Trust (WoT) を用いた．PGP は暗号化プログラムであり，WoT は PGP 公開鍵の信頼性を非中央集権的な方法で担保するための仕組みである [15]．WoT の形成するネットワークは現実世界における人同士の信頼関係ネットワークの部分グラフであり，公開鍵の所有者はノードに，公開鍵に対するデジタル署名がエッジに対応する．

(注1)：実際の Freenet の実装においてはリクエストの発信者やデータの保持者の匿名性を保つために，TTL が最大値または 1 の場合は TTL の減少が確率的に行われる．詳細は [4] 等を参照．

京都大学 KYOTO UNIVERSITY
A Self-archived copy in
Kyoto University Research Information Repository
https://repository.kulib.kyoto-u.ac.jp
京都大学学術情報リポジトリ KURENAI 紅 Kyoto University Research Information Repository

WoT は本来有向グラフであるが, 先行研究に従い「公開鍵の所有者間で相互にデジタル署名が行われている」ことを「ノード間に信頼がある」と定義する. よって元のネットワークデータから単方向の署名に対応するエッジを削除したものから giant component (最もノード数の多い連結部分グラフ) を抽出することによって得られたグラフを信頼関係ネットワーク $G = (V, E)$ とする. ここで G は無向グラフと見なすことができる.

総ノード数 $\|V\|$	48983
総エッジ数 $\|E\|$	183840
平均最短経路長	6.60
直径	35
平均次数	7.51
最大次数	885
クラスタリング係数	0.31
スケーリング指数	1.92

表 1　2016 年 12 月 11 日時点における Web of Trust の基本情報
使用データセット: `https://wot.siccegge.de/download/2016-12-11.wot`

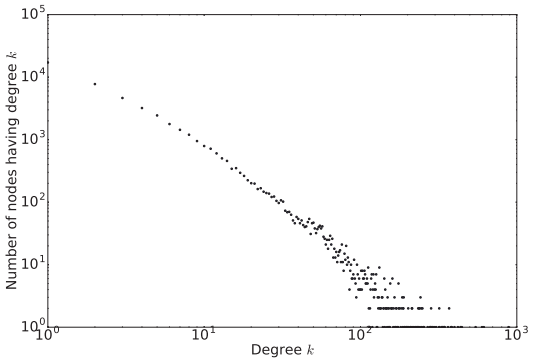

図 3　Web of Trust ネットワークの次数分布

WoT G の解析の結果判明したネットワークの特徴を表 1 に示す. なお平均最短経路長は Dijkstra 法により, スケーリング指数については最小二乗法により求めた. 表 1 と WoT の次数分布をプロットした図 3 に見られるように, 高いクラスタリング係数, 小さな平均最短経路長, べき則に従う次数分布等, 典型的なスモールワールドネットワークかつスケールフリーネットワークの特徴が確認できる.

WoT をシミュレーション用実データとして用いている [7] や [6] では以上に述べたのと同様の前処理の後さらにネットワークの局所的な部分グラフを取り出したり, 低次数ノードを削除するなどの操作を加えた後シミュレーションを行っているが, 本研究では現実の F2F ネットワークトポロジーにおけるルーティングのパフォーマンスをより正確に評価するために, そういった意図的な操作は施さずにシミュレーションを行った.

なお今回行ったシミュレーションに関わる全てのソースコードは GitHub レポジトリ (`https://github.com/akiratk0355/navigable-network-analysis`) にて閲覧可能である.

5.3　シミュレーション結果

まず WoT ネットワークに SWAP アルゴリズムを適用し, ID 空間に埋め込んだ様子を図 4 に示す. Kleinberg モデルによって生成されたグラフと同様に「距離が近いノードどうしほどエッジを持ちやすい」という特徴が現れており, Kleinberg モデルの性質が「復元」されたのが視覚的にも確認出来る.

また local contact の存在率を p_{local} =(ID 空間上で最も近距離にいるノード同士を接続するエッジの本数)/$|V|$ と定義し, 初期状態と SWAP アルゴリズム適用後のグラフについてそれぞれ p_{local} を算出した. その結果ランダムに ID を割り当てた初期状態において $p_{\mathrm{local}} = 0.0002$ だったのに対し, 図 4 では $p_{\mathrm{local}} = 0.23$ と大幅に改善してはいるものの, 1.0 からは程遠いため, 埋め込み後のネットワークにおける単純な greedy ルーティングの効率性が担保されないことが, この時点ですでに予測される.

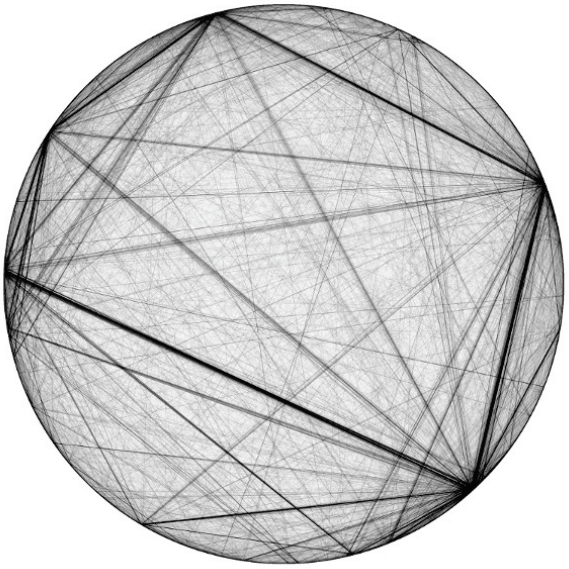

図 4　SWAP アルゴリズムにより ID 空間 $[0, 1)$ に埋め込まれた Web of Trust ネットワーク

次に図 4 のネットワークに対するルーティングシミュレーションを行った結果を表 2 と図 5 に示す. シミュレーションの結果 D^3-DFS は D^2-DFS を 15%以上成功率で上回り, にも関わらず平均ホップ数を 20 以上短縮するという大幅なパフォーマンスの改善を見せた. また図 5 の通り, TTL を 500 以下のどのような値に設定したとしても, D^3-DFS が既存アルゴリズムよりも高い成功率を実現することが可能であることを確認できた.

	D^2-DFS	D^3-DFS
成功率	0.23	0.38
平均ホップ数	87	64

表 2　ID 割り当て後の Web of Trust ネットワークにおける各ルーティングアルゴリズムの成功率と平均ホップ数

京都大学 KYOTO UNIVERSITY
A Self-archived copy in
Kyoto University Research Information Repository
https://repository.kulib.kyoto-u.ac.jp
京都大学学術情報リポジトリ KURENAI 紅 Kyoto University Research Information Repository

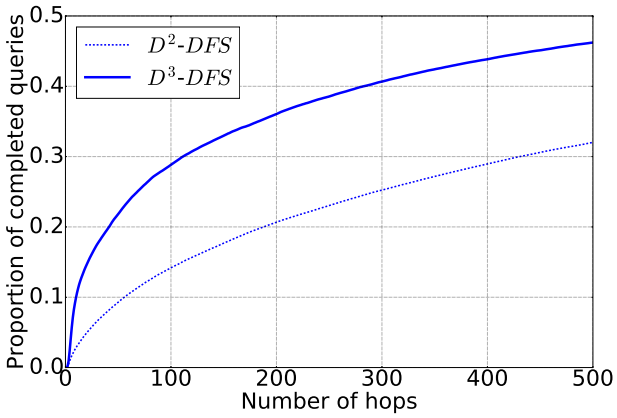

図 5　ID 割り当て後の Web of Trust ネットワークにおける各ホップ数以下で成功したルーティング試行の割合

6. まとめと今後の課題

本研究では F2F ネットワークにおける分散ルーティングの手法として主に Freenet のプロトコルを概観した．そして Sandberg の埋め込み生成アルゴリズムを Web of Trust ネットワークデータに適用し，ルーティングシミュレーションを行うことにより，ピュアな F2F ネットワークトポロジーにおける従来のルーティングアルゴリズムのパフォーマンスを実証的に確認した．

その上で分散ルーティングの効率性を向上させるために D^2-DFS に隣接ノードの次数を考慮したヒューリスティックを加えた D^3-DFS を提案し，そのパフォーマンス評価を行った．その結果 D^3-DFS が D^2-DFS を成功率や平均ホップ数の面で凌ぐことが確認できた．よって Freenet の実装においても D^3-DFS がルーティング機能を改善できるのではないかと期待できる．直近の展望としては，バックトラッキングの回数比較等アルゴリズムの詳細な挙動分析を始めとして，ハブノードがダウンした状況下でのルーティング実験，データの insert/request 実験，接続先を限定しないノード (Opennet ノード) の存在を考慮した実験等 Freenet の実装により近い状況下におけるパフォーマンス評価が挙げられる．

ただし今回の実験における D^3-DFS は成功率が 40%弱であり，それ自体決して高い値とは言えない．また表 1 の通り今回用いた Web of Trust ネットワークにおける本来の平均最短経路長が 6.60 であるの対し，D^3-DFS の平均ホップ数は依然 60 以上と最適値には程遠い．P2P ネットワークへの応用を考えた場合，ノード間の通信効率を保証するためにも他ノード到達の成功率を高く保ちホップ数を抑えることは非常に重要であるため，これらのパフォーマンス指標をさらに改善させることが，ピュアな F2F ネットワークを実用的なレベルにまで押し上げるための今後の課題である．例えば今回次ノード選択のヒューリスティックに EVN を用いたが，更に高いパフォーマンスを発揮するヒューリスティックを今後模索すべきであろう．また今回埋め込みアルゴリズムは先行研究の SWAP をそのまま用いたが，greedy ルーティングが効率的となる様々な埋め込みのアルゴリズムが他にも提案されている．よって他の埋め込みアルゴリズムを適用した後のネットワークにおいて D^3-DFS が更に良いパフォーマンスを発揮できるか否か検証するべきだろう．

文　献

[1] G. Greenwald, E. MacAskill, and L. Poitras, “Edward Snowden: the whistleblower behind the NSA surveillance revelations,” 2013. https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance
[2] D. Bricklin, “Friend-to-friend networks,” http://www.bricklin.com/f2f.htm, 2000.
[3] M. Rogers and S. Bhatti, “How to disappear completely: A survey of private peer-to-peer networks,” networks, vol.13, p.14, 2007.
[4] D.-M.S. Roos, “Analyzing and enhancing routing protocols for friend-to-friend overlays,” PhD thesis, TU Dresden, Germany, 2016.
[5] I. Clarke, O. Sandberg, B. Wiley, and T.W. Hong, “Freenet: A distributed anonymous information storage and retrieval system,” Designing Privacy Enhancing TechnologiesSpringer, pp.46–66 2001.
[6] I. Clarke, O. Sandberg, M. Toseland, and V. Verendel, “Private communication through a network of trusted connections: The dark freenet,” https://freenetproject.org/assets/papers/freenet-0.7.5-paper.pdf, 2010.
[7] O. Sandberg, “Distributed routing in small-world networks,” Proceedings of the Meeting on Algorithm Engineering & ExpermimentsSociety for Industrial and Applied Mathematics, pp.144–155 2006.
[8] J. Kleinberg, “The small-world phenomenon: An algorithmic perspective,” Proceedings of the thirty-second annual ACM symposium on Theory of computingACM, pp.163–170 2000.
[9] N.S. Evans, C. GauthierDickey, and C. Grothoff, “Routing in the dark: Pitch black,” Computer Security Applications Conference, 2007. ACSAC 2007. Twenty-Third AnnualIEEE, pp.305–314 2007.
[10] Ö. Şimşek and D. Jensen, “Navigating networks by using homophily and degree,” Proceedings of the National Academy of Sciences, vol.105, no.35, pp.12758–12762, 2008.
[11] S. Milgram, “The Small World Problem,” Psychology Today, vol.2, pp.60–67, 1967.
[12] C.H. Papadimitriou and D. Ratajczak, “On a conjecture related to geometric routing,” Theoretical Computer Science, vol.344, no.1, pp.3–14, 2005.
[13] S. Roos and T. Strufe, “Dealing with dead ends: Efficient routing in darknets,” ACM Transactions on Modeling and Performance Evaluation of Computing Systems, vol.1, no.1, p.4, 2016.
[14] B. Schiller, S. Roos, A. Hofer, and T. Strufe, “Attack resistant network embeddings for darknets,” Reliable Distributed Systems Workshops (SRDSW), 2011 30th IEEE Symposium onIEEE, pp.90–95 2011.
[15] P.R. Zimmermann, The official PGP user’s guide, MIT press, 1995.